Electronic Colloquium on Computational Complexity, Report No. 18 (2009)

$GF(2^n)$-Linear Tests versus $GF(2)$-Linear Tests*

Yoav Tzur†

March 8, 2009

Abstract

A small-biased distribution of bit sequences is defined as one withstanding $GF(2)$-linear tests for randomness, which are linear combinations of the bits themselves. We consider linear combinations over larger fields, specifically, $GF(2^n)$ for n that divides the length of the bit sequence. Indeed, this means that we partition the bits to blocks of length n and treat each block as the representation of a field element. Various properties of the resulting field element can then be tested. We show that the latter $GF(2^n)$-linear tests are at least as powerful as the $GF(2)$-linear tests. This holds even for a very limited final test of the resulting field element (e.g., checking only the first bit). This is shown constructively in the sense that we show for each linear combination over $GF(2)$, an explicit linear combination over $GF(2^n)$ whose first bit (for instance) has the same bias.

One corollary of the above is that the generator producing a random geometric series over $GF(2^n)$, namely $(a, b) \mapsto (a^i \cdot b)_{i=0}^{\ell}$, is $\frac{\ell}{2^n}$-biased.

Given the technical nature of the current work, we start with the formal setting (Section 1), to be followed by a discussion (Section 2). The proof of the main result appears in section 3.

1 Formal Setting

We start with the notion of ε-bias, introduced in [7], which refers to $GF(2)$-linear tests:

Definition 1 (ε-bias)**.** *For $\varepsilon > 0$, $k, \ell \in \mathbb{N}$, a generator $G : \{0,1\}^k \to \{0,1\}^\ell$ is called* ε-biased *if for every nontrivial $GF(2)$-linear combination $\alpha \in \{0,1\}^\ell$,*

$$\Pr_{s \in \{0,1\}^k}[\langle G(s), \alpha \rangle = 0] = \frac{1}{2} \pm \varepsilon.$$

*This research was partially supported by the Israel Science Foundation (grant No. 1041/08).

†Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. Email: yoav.tzur@weizmann.ac.il.

ISSN 1433-8092

(For two vectors x, y, we denote by $\langle x, y\rangle$ their inner product $x^T y$.)
The bits of $G(s)$, for s uniformly distributed in $\{0,1\}^k$, are called ε-biased.

In order to introduce $GF(2^n)$-linear tests and study them, we will use the following notation:

Notation. *For a vector $a \in \{0,1\}^n$, we will usually denote by $\tilde{a}$ the $GF(2^n)$ element represented by a. When writing an expression in $GF(2^n)$ elements (denoted by a tilde), the arithmetic will usually be that of $GF(2^n)$; otherwise (when elements are without a tilde), we treat them as vectors in $\{0,1\}^n$ and use the arithmetic of the vector space (over $GF(2)$).*

Definition 2 (ε-resilience under $GF(2^n)$-linear tests)**.** *For $\varepsilon > 0$, $n, k, \ell \in \mathbb{N}$, a generator $G : \{0,1\}^{k\cdot n} \to \{0,1\}^{(\ell+1)\cdot n}$ is called* ε-resilient under $GF(2^n)$-linear tests *if for every nontrivial $GF(2^n)$-linear combination, $\tilde{b}_i \in GF(2^n)$ for $i = 0...\ell$, the distribution induced by the sum $\sum_{i=0}^{\ell} \tilde{b}_i \cdot \tilde{g}_i(s)$ over a random seed s is ε-close to the uniform distribution over $GF(2^n)$, where $g_i(s)$ denotes the i-th block of length n in the output $G(s)$ and $\tilde{g}_i(s)$ is the $GF(2^n)$ element it represents. That is, for every set $B \subseteq GF(2^n)$, it holds that*

$$\left| \Pr_s \left[\sum_{i=0}^{\ell} \tilde{b}_i \cdot \tilde{g}_i(s) \in B \right] - \frac{|B|}{2^n} \right| \leq \varepsilon. \tag{1}$$

A weaker definition that only considers a specific set B is:

Definition 3 ((ε, B)-resilience under $GF(2^n)$-linear tests)**.** *For $\varepsilon > 0$, $n, k, \ell \in \mathbb{N}$ and $B \subseteq GF(2^n)$, a generator $G : \{0,1\}^{k\cdot n} \to \{0,1\}^{(\ell+1)\cdot n}$ is called* (ε, B)-resilient under $GF(2^n)$-linear tests *if for every nontrivial $GF(2^n)$-linear combination, $\tilde{b}_i \in GF(2^n)$ for $i = 0...\ell$, Equation (1) holds.*

So a generator is ε-resilient under $GF(2^n)$-linear tests if and only if, for any $B \subseteq GF(2^n)$, the generator is (ε, B)-resilient under $GF(2^n)$-linear tests. If we consider only all sets B that are linear subspaces of co-dimension 1, i.e. sets of the form $\Gamma = \{\tilde{a} : \gamma^T a = 0\}$ for some nonzero vector $\gamma \in \{0,1\}^n$, we actually require the n bits representing the resulting field element to be ε-biased. This case is referred to as *ε-linear-resilience*:

Definition 4 (ε-linear-resilience under $GF(2^n)$-linear tests)**.** *For $\varepsilon > 0$, $n, k, \ell \in \mathbb{N}$, a generator $G : \{0,1\}^{k\cdot n} \to \{0,1\}^{(\ell+1)\cdot n}$ is called* ε-linear-resilient under $GF(2^n)$-linear tests *if for every nonzero vector $\gamma \in \{0,1\}^n$, it holds that G is (ε, Γ)-resilient under $GF(2^n)$-linear tests, where $\Gamma = \{\tilde{a} : \gamma^T a = 0\} \subseteq GF(2^n)$. That is, for every nontrivial $GF(2^n)$-linear combination, $\tilde{b}_i \in GF(2^n)$ for $i = 0...\ell$, the distribution induced by $\sum_{i=0}^{\ell} \tilde{b}_i \cdot \tilde{g}_i(s)$ over a random seed s is ε-biased when viewed as the sequence of bits representing the resulting $GF(2^n)$-element.*

Clearly, for $n = 1$ the above three definitions (with nontrivial B in Definition 3) coincide with the notion of ε-bias.

Our main result, proven in Section 3, is the following "reduction":

Theorem 5 (Main Theorem)**.** *For $\varepsilon > 0$, $n \in \mathbb{N}$, and for any nonzero vector $\gamma \in \{0,1\}^n$, if G is (ε, Γ)-resilient under $GF(2^n)$-linear tests, where $\Gamma = \{\tilde{a} : \gamma^T a = 0\}$, then G is is ε-biased.*

The converse of Theorem 5 is immediate, since each bit in the representation of $\sum_{i=0}^{\ell} \tilde{b}_i \cdot \tilde{g}_i(s)$ is a linear combination in the bits of $G(s)$.[1] Since both Theorem 5 and its converse hold for any nonzero γ, we get that ε-linear-resilience under $GF(2^n)$-linear tests is equivalent to ε-bias. Note that this holds for *any* n that divides the output length of the generator.

Since being ε-resilient under $GF(2^n)$-linear tests implies being ε-linear-resilient under $GF(2^n)$-linear tests (every set Γ as in Definition 4 qualifies as a set B of size 2^{n-1} in Definition 2), Theorem 5 also yields:

Corollary 6. *For $\varepsilon > 0$, $n \in \mathbb{N}$, a generator G that is ε-resilient under $GF(2^n)$-linear tests is ε-biased.*

We note that the converse of Corollary 6 does not hold, but it is known that being ε-biased implies being $2^{n/2} \cdot \varepsilon$-resilient under $GF(2^n)$-linear tests (see [6]).

2 Discussion

One concrete motivation to Definitions 2 and 4 is their role in the following two-step methodology for constructing natural small-bias generators based on $GF(2^n)$-sequences: first show that the generator is resilient under $GF(2^n)$-linear tests (resp., linear-resilient under $GF(2^n)$-linear tests), and next use Corollary 6 (resp., Theorem 5) to conclude that it has small bias. To demonstrate this methodology we consider the following generator that produces random geometric sequences (i.e., on seed $a, b \in \{0,1\}^n$, we output the sequence $\tilde{a}^i \tilde{b}$ for $i = 0, 1, ..., \ell$). We note that this generator was considered in [3], where it was implicitly proven to have small bias (see further discussion below).

Proposition 7. *For $n, \ell \in \mathbb{N}$, the generator $G : \{0,1\}^{2n} \to \{0,1\}^{(\ell+1)\cdot n}$ defined by $\tilde{g}_i(a,b) = \tilde{a}^i \cdot \tilde{b}$ is $\frac{\ell}{2^n}$-resilient under $GF(2^n)$-linear tests, where $\tilde{a}, \tilde{b}$ are the $GF(2^n)$ elements represented by a, b, respectively, and $g_i(a,b)$ is the representation of $\tilde{g}_i(a,b)$.*

Proof. Fix any nontrivial $GF(2^n)$-linear combination $(\tilde{c}_i)_{i=0}^{\ell}$, and any set $B \subseteq GF(2^n)$, and consider

$$\Pr_{a,b}\left[\sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{a}^i \tilde{b} \;\in\; B\right] \quad = \quad \Pr_{a,b}\left[\left(\tilde{b} \cdot \sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{a}^i\right) \;\in\; B\right].$$

[1] If M_{b_i} is the linear operator over $\{0,1\}^n$ that performs multiplication by $\tilde{b}_i$, then $\gamma^T \sum_{i=0}^{\ell} M_{b_i} g_i(s)$ is clearly a linear combination in the bits of $G(s) = (g_0(s), g_1(s), ..., g_\ell(s))$. For details regarding the matrix M_{b_i}, see the second Notation paragraph of Section 3.

When $\sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{a}^i$ is nonzero, $\tilde{b} \cdot \sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{a}^i$ is uniformly distributed in $GF(2^n)$. Thus, the statistical difference (referred to in Equation (1)) is

$$\left| \Pr_{a,b}\left[\sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{a}^i \tilde{b} \ \in \ B \right] - \frac{|B|}{2^n} \right| \leq \Pr_{a}\left[\sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{a}^i = 0 \right] \leq \frac{\ell}{2^n},$$

where the second inequality holds since the nonzero (degree $\leq \ell$) polynomial $\sum_{i=0}^{\ell} \tilde{c}_i \cdot \tilde{x}^i$ can have at most ℓ roots (in $GF(2^n)$). $\square$

By Corollary 6, we immediately get:

Corollary 8. *For $n, \ell \in \mathbb{N}$, the generator $G : \{0,1\}^{2n} \to \{0,1\}^{(\ell+1)\cdot n}$ defined by $\tilde{g}_i(a,b) = \tilde{a}^i \cdot \tilde{b}$ is $\frac{\ell}{2^n}$-biased (with respect to $GF(2)$-linear tests).*

This result can be contrasted with the similar Construction 3 in [1], in which for $i = 0 \ldots \ell$, the element $\tilde{a}$ is raised to the i-th power, but then an inner product with b is taken, rather than their $GF(2^n)$-product, producing a single bit. The construction here seems slightly more natural and simple.

As further motivation for our definitions, we note that [3] uses the construction of Proposition 7 for obtaining a graph with normalized second eigenvalue $\frac{\ell}{2^n}$. Their argument implicitly shows that any ε-linear-resilient[2] generator under $GF(2^n)$-linear tests yields a Cayley graph with normalized second eigenvalue of 2ε (The case of $n = 1$ was previously shown in [2]). Indeed, in [3] this is done directly (and not by using a reduction similar to our Theorem 5). However, Theorem 5 can be (non-constructively) derived by combining the above claim (i.e., ε-linear-resilience under $GF(2^n)$-linear tests implies (normalized) second eigenvalue 2ε) with its converse for the case of $n = 1$. We mention that the converse for $n = 1$ was known before, and can be derived for any n by reversing the argument of [3].

3 Proof of Theorem 5

A nonconstructive proof of Theorem 5 can be understood while skipping all preliminaries and starting with Lemma 15.

3.1 Preliminaries

To prove our main theorem, we first present some notation and known algebraic facts that we need.

Notation. *We will use the standard representation of $GF(2^n)$ as $GF(2)[x]/(c(x))$, fixing an irreducible polynomial $c(x) \in GF(2)[x]$ of degree n. An element*

[2] Or even, in fact, any (ε, Γ)-resilient generator under $GF(2^n)$-linear tests for any nontrivial $\Gamma \subseteq GF(2^n)$ which is a linear subspace over $\{0,1\}$ of co-dimension 1 (i.e., $\Gamma = \{\tilde{a} : \gamma^T a = 0\}$ for some nonzero $\gamma \in \{0,1\}^n$).

$\tilde{a} \in GF(2^n)$, represented by the bit string $a = a_0a_1...a_{n-1}$, corresponds to $p_a(x) = \sum_{i=0}^{n-1} a_i x^i \in GF(2)[x]/(c(x))$. Denote by C the companion matrix of $c(x)$, with ones under the diagonal and the coefficients $c_0, ..., c_{n-1}$ in the right column:

$$C = \begin{pmatrix} 0 & 0 & \dots & c_0 \\ 1 & 0 & \dots & c_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & c_{n-1} \end{pmatrix}$$

Note that for an element $\tilde{b} \in GF(2^n)$ represented by $b \in \{0,1\}^n$, the vector $C \cdot b$ corresponds to multiplying p_b by the fixed polynomial x (represented by the bit-string $e_2 = 010...0$) and reducing the result modulo $c(x)$, i.e. $C \cdot b$ represents the multiplication $\tilde{e}_2 \cdot \tilde{b}$.

As noted earlier, we use vectors and matrices over $\{0,1\}$, and use the tilde when we want to refer to the $GF(2^n)$-elements represented. However, when needed, we will sometimes use the larger vector space $GF(2^n)^n$, and work with matrices and vectors over $GF(2^n)$. In such cases, we will note this explicitly.

Fact 9. *The eigenvalues of C (over $GF(2^n)$) are exactly the roots of $c(x)$. Moreover, if $c(x)$ has n distinct roots $\lambda_1, ..., \lambda_n \in GF(2^n)$, it is diagonalizable as $C = V^{-1} \cdot \mathrm{diag}(\lambda_1, ..., \lambda_n) \cdot V$, with $\mathrm{diag}(\lambda_1, ..., \lambda_n)$ denoting the diagonal matrix with λ_i in the ii-th entry, and V being the Vandermonde matrix defined as $[V]_{ij} = \lambda_{i+1}^j$, for $i, j = 0, ..., n-1$. (Note: the entries of V are in $GF(2^n)$. Although the matrices in the expression have entries in $GF(2^n)$, the matrix C is over $GF(2)$.)*

Fact 9 is a direct corollary of the transposed version of Theorem 6.13 in [5], applying the same arguments to $GF(2^n)$ rather than to the complex field $\mathbb{C}$.

Notation. *Define $M_a = p_a(C)$. This is the linear operator that performs multiplication by $\tilde{a}$ on elements viewed as n-dimensional vectors over $GF(2)$. That is, for every $\tilde{b} \in GF(2^n)$, represented by the vector $b \in \{0,1\}^n$, the binary representation of the element $\tilde{a} \cdot \tilde{b}$ is $M_a \cdot b$. To see this, write $p_a(C) \cdot b = \sum_i a_i C^i b$, and note that this vector represents the reduction of $\sum_i a_i p_b(x) \cdot x^i = \sum_{i,j} a_i b_j x^{i+j}$ modulo $c(x)$, which indeed corresponds to multiplying $\tilde{b}$ by $\tilde{a}$ in the field.*

Fact 10. *Every irreducible polynomial over a finite field has no multiplied roots.*

Fact 10 appears as a note in Section XV.6 of [4], at the end of page 413.

Corollary 11. *For any $\tilde{a} \in GF(2^n)$, it holds that $M_a = V^{-1} \cdot \mathrm{diag}(p_a(\lambda_1), ..., p_a(\lambda_n)) \cdot V$. (Note: although the matrices in the expression have entries in $GF(2^n)$, the matrix M_a is over $GF(2)$.)*

Proof. By Fact 10, $c(x)$ has distinct roots. We thus write C using Fact 9 as $V^{-1} \cdot \mathrm{diag}(\lambda_1, ..., \lambda_n) \cdot V$. Observe that $C^i = \left(V^{-1} \cdot \mathrm{diag}(\lambda_1, ..., \lambda_n) \cdot V\right)^i =$

$V^{-1} \cdot \mathrm{diag}(\lambda_1^i, ..., \lambda_n^i) \cdot V$, and for $\tilde{a} \in GF(2^n)$ we have

$$\begin{aligned} M_a &= p_a(C) \\ &= \sum_{i=0}^{n-1} a_i C^i \\ &= \sum_{i=0}^{n-1} a_i \cdot V^{-1} \cdot \mathrm{diag}(\lambda_1^i, ..., \lambda_n^i) \cdot V \\ &= V^{-1} \left(\sum_{i=0}^{n-1} a_i \,\mathrm{diag}(\lambda_1^i, ..., \lambda_n^i) \right) V \\ &= V^{-1} \cdot \mathrm{diag}(p_a(\lambda_1), ..., p_a(\lambda_n)) \cdot V. \end{aligned}$$

□

Fact 12. *Every symmetrical multinomial $p(x_1, ..., x_n)$ over a field F, evaluated on the roots $\lambda_1, ..., \lambda_n$ of any polynomial $q(x)$ over F (the roots possibly in a larger algebraic extension of F), takes value in F.*

Fact 12 is Theorem 10 in Section XV.4 of [4].

3.2 The Core of Our Proof

Using Fact 12, it follows that while the entries of V are in $GF(2^n)$, the entries of $V^T V$ (and its inverse) are in $GF(2)$:[3]

Corollary 13. *The entries of $V^T V$ are all in $GF(2)$.*

Proof. The ij-th entry of $V^T V$ is $\sum_{k=0}^{n-1} V_{ik}^T V_{kj} = \sum_{k=0}^{n-1} \lambda_{k+1}^{i+j}$. For any fixed i, j this is a symmetric polynomial over $GF(2)$, evaluated on the roots of $c(x)$. So by Fact 12, it takes value in the base field $GF(2)$. □

Define $U = V^{-1} \cdot {V^{-1}}^T$. By Corollary 13, the entries of U^{-1} and U are in $GF(2)$. These matrices allow to replace M_a^T by M_a as follows:

Claim 14. *For every $a \in \{0,1\}^n$, it holds that $M_a^T = U^{-1} M_a U$.*

Proof. Using the diagonalization from Corollary 11, we have $M_a = V^{-1}\,\mathrm{diag}(p_a(\lambda_1), ..., p_a(\lambda_n))V$ and so

$$\begin{aligned} U^{-1} M_a U &= V^T V \cdot V^{-1}\,\mathrm{diag}(p_a(\lambda_1), ..., p_a(\lambda_n)) V \cdot V^{-1} {V^{-1}}^T \\ &= V^T\,\mathrm{diag}(p_a(\lambda_1), ..., p_a(\lambda_n))^T {V^{-1}}^T \\ &= M_a^T. \end{aligned}$$

□

[3] Actually, Corollary 13 requires very little from the polynomial $c(x)$: any Vandermonde matrix V of the roots of a degree n polynomial would have the entries of $V^T V$ in the base field.

The following lemma captures the core of our argument. It says that the i-th bit of the representation of $\tilde{a} \cdot \tilde{b}$ can be written as the inner product of $Q \cdot a$ and b, where Q is a fixed matrix over $GF(2)$. The statement generalizes to any fixed linear combination in the representation of $\tilde{a} \cdot \tilde{b}$, denoted γ (where the aforementioned case corresponds to $\gamma = e_i$).

Lemma 15. *For every fixed linear combination $\gamma \in \{0,1\}^n$, there exists a matrix $Q_\gamma \in \{0,1\}^{n \times n}$ such that for every two vectors $u, v \in \{0,1\}^n$:*

$$\langle \gamma, M_u \cdot v \rangle = \langle Q_\gamma \cdot u, v \rangle = v^T Q_\gamma u.$$

Moreover, Q_γ is invertible whenever γ is nonzero.

We present a simple nonconstructive proof as well as a constructive proof giving an explicit expression for Q_γ.

Proof (nonconstructive). Fixing γ, the value $\langle \gamma, M_u \cdot v \rangle$ is a quadratic form in the bits of u and v and thus can be represented as $v^T Q_\gamma u$ for some matrix Q_γ. For the moreover part, let d satisfy $\gamma^T d = 1$ (e.g., if the i-th bit of γ is 1, set $d = e_i$). Then, for every nonzero $u \in \{0,1\}^n$, setting v_u to represent $\tilde{u}^{-1}\tilde{d} \in GF(2^n)$, we get $\langle Q_\gamma \cdot u, v_u \rangle = \langle \gamma, M_u \cdot v_u \rangle = \langle \gamma, d \rangle = 1$ and so $Q_\gamma \cdot u$ cannot be the zero vector. This implies that the kernel of Q_γ is trivial. $\square$

Proof (constructive). For U as defined above, given $\gamma \in \{0,1\}^n$, we set $Q_\gamma = U^{-1} M_{U\gamma}$. Recall that if $\tilde{d} \in GF(2^n)$ is the element represented by the vector $d = U \cdot \gamma \in \{0,1\}^n$, then $M_{U\gamma} = M_d$ is the matrix corresponding to the linear transformation over $\{0,1\}^n$ that maps the representation a of the element $\tilde{a} \in GF(2^n)$ to the representation of $\tilde{d} \cdot \tilde{a} \in GF(2^n)$. We get:

$$\begin{aligned}
\langle \gamma, M_u v \rangle &= \left\langle M_u^T \gamma, v \right\rangle \\
\text{(by Claim 14)} \qquad &= \left\langle U^{-1} M_u U \gamma, v \right\rangle \\
\text{(by commutativity of } GF(2^n)\text{)} \qquad &= \left\langle U^{-1} M_{U\gamma} \cdot u, v \right\rangle \\
&= \langle Q_\gamma \cdot u, v \rangle .
\end{aligned}$$

The moreover part follows from the invertibility of U and $M_{U\gamma}$ when $\gamma \neq 0$. $\square$

3.3 Finishing the Proof

Finally, we get to actually proving Theorem 5:

Proof of Theorem 5. Fix a nonzero $\gamma \in \{0,1\}^n$, and let $G : \{0,1\}^{k \cdot n} \to \{0,1\}^{(\ell+1) \cdot n}$ be an (ε, Γ)-resilient generator under $GF(2^n)$-linear tests, where $\Gamma = \{\tilde{a} : \gamma^T a = 0\}$. Fix an arbitrary linear combination $\bar{\alpha} \in \{0,1\}^{(\ell+1)n}$ on the bits of G, and parse it to $\ell + 1$ vectors $\alpha_0, ..., \alpha_\ell \in \{0,1\}^n$. Define a series of $GF(2^n)$ elements $\tilde{b}_0, ..., \tilde{b}_\ell \in GF(2^n)$, represented by the vectors $b_i = Q_\gamma^{-1} \alpha_i$ for

$i = 0, ..., \ell$, where Q_γ is the matrix guaranteed by Lemma 15. We get that for any output of the generator G, denoted $(g_0, ..., g_\ell) \in \{0,1\}^{(\ell+1)n}$:

$$\sum_{i=0}^{\ell} \langle \alpha_i, g_i \rangle \underset{\text{Def. of } b_i}{\underset{\uparrow}{=}} \sum_{i=0}^{\ell} \langle Q_\gamma b_i, g_i \rangle \underset{\text{Lemma 15}}{\underset{\uparrow}{=}} \sum_{i=0}^{\ell} \langle \gamma, M_{b_i} g_i \rangle = \gamma^T \sum_{i=0}^{\ell} M_{b_i} g_i.$$

Recalling the definition of Γ, we get that

$$\Pr_s [\langle \bar{\alpha}, G(s) \rangle = 0] = \Pr_s \left[\sum_{i=0}^{\ell} \langle \alpha_i, g_i(s) \rangle = 0 \right] = \Pr_s \left[\gamma^T \sum_{i=0}^{\ell} M_{b_i} g_i(s) = 0 \right] = \Pr_s \left[\sum_{i=0}^{\ell} \tilde{b}_i \cdot \tilde{g}_i(s) \in \Gamma \right].$$

Assuming $\bar{\alpha} \neq 0^{(\ell+1)\cdot n}$, there exists an i such that $\alpha_i \neq 0^n$ and so $\tilde{b}_i$, represented by the vector $Q_\gamma^{-1} \alpha_i$ is nonzero. Now, the right hand side is bounded by the (ε, Γ)-resilience of G under $GF(2^n)$-linear tests, giving the same bound on the left hand side. This completes the proof. □

An interesting corollary to Lemma 15 is that any linear combination in the bits of any b can be computed as a prefixed linear combination in the bits of the representation of $\tilde{a} \cdot \tilde{b}$ for a suitable choice of $\tilde{a} \in GF(2^n)$.

Corollary 16. *For every nonzero $\alpha, \gamma \in \{0,1\}^n$ there exists $b \in \{0,1\}^n$ such that for every $g \in \{0,1\}^n$, it holds that $\langle \alpha, g \rangle = \langle \gamma, M_b \cdot g \rangle$.*

Proof. Set $b = Q_\gamma^{-1} \alpha$. By Lemma 15, $\langle \gamma, M_b \cdot g \rangle = \langle Q_\gamma \cdot b, g \rangle = \langle \alpha, g \rangle$. □

Corollary 16 can be seen as an interpretation for the proof of Theorem 5: every inner product $\langle \alpha_i, g_i \rangle$ is calculated as $\langle \gamma, M_{b_i} \cdot g_i \rangle$ for the adequate b_i that depends on α_i and γ; linearity of the inner products is then used to give $\sum_{i=0}^{\ell} \langle \alpha_i, g_i \rangle = \left\langle \gamma, \sum_{i=0}^{\ell} M_{b_i} \cdot g_i \right\rangle$.

4 Acknowledgements

I would like to thank my advisor, Oded Goldreich, for very helpful ideas, comments and observations. I also thank Noga Alon for useful conversations that brought to simplifications of the claims and proofs.

References

[1] N. Alon, O. Goldreich, J. Hastad and R. Peralta, "Simple Constructions of Almost k-wise Independent Random Variables", *Random Structures and Algorithms*, vol. 3, pp. 289–304, 1992.

[2] N. Alon and Y. Roichman, "Random Cayley Graphs and Expanders", *Random Structures and Algorithms*, vol. 5, pp. 271–284, 1994.

[3] N. Alon, O. Schwartz and A. Shapira, "An Elementary Construction of Constant-Degree Expanders", In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, 2007.

[4] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, third edition, MacMillan, New York, 1965.

[5] H. Dym, *Linear Algebra in Action*, AMS Bookstore, 2007.

[6] O. Goldreich, "Three XOR-Lemmas - an Exposition", *Electronic Colloquium on Computational Complexity*, TR 95-050, 1995.

[7] J. Naor and M. Naor, "Small-Bias Probability Spaces: Efficient Constructions and Applications", *SIAM Journal on Computing*, vol. 22, pp. 838–856, 1993.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/